UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/026,813 | 12/27/2001 | Hiroo Nakano | 217781US2S | 1908 |

22850 7590 12/15/2006

C. IRVIN MCCLELLAND
OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

| EXAMINER | |
|---|---|
| HOFFMAN, BRANDON S | |
| ART UNIT | PAPER NUMBER |
| 2136 | |

DATE MAILED: 12/15/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

Application Number: 10/026,813
Filing Date: December 27, 2001
Appellant(s): NAKANO, HIROO



Zachary Stern (U.S. Reg. No. 54,719)
For Appellant

**EXAMINER'S ANSWER**

This is in response to the appeal brief filed September 21, 2006, appealing from the Office action mailed November 7, 2005.

**(1) Real Party in Interest**

A statement identifying by name the real party in interest is contained in the brief.

**(2) Related Appeals and Interferences**

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

**(3) Status of Claims**

The statement of the status of claims contained in the brief is correct.

**(4) Status of Amendments After Final**

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

**(5) Summary of Claimed Subject Matter**

The summary of claimed subject matter contained in the brief is correct.

**(6) Grounds of Rejection to be Reviewed on Appeal**

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

**(7) Claims Appendix**

The copy of the appealed claims contained in the Appendix to the brief is correct.

**(8) Evidence Relied Upon**

| | | |
|---|---|---|
| 6,839,849 | Ugon et al. | 1-2005 |
| 6,698,662 | Feyt et al. | 3-2004 |

**(9) Grounds of Rejection**

The following ground(s) of rejection are applicable to the appealed claims:

***Claim Rejections - 35 USC § 103***

Claims 1-4 and 11-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ugon et al. (U.S. Patent No. 6,839,849) in view of Feyt et al. (U.S. Patent No. 6,698,662).

Regarding claims 1, 3, 11 and 13, Ugon teaches a data processing apparatus/memory card comprising:

- An operation processing unit (fig.1 item 1) having at least a read cycle period when said operation processing unit reads data from a device (col. 5, lines 65-67), and a write cycle period when said operation processing unit writes data in the device (col. 6, lines 2-5);
- A memory which performs data transmission/reception between said operation processing unit and said memory (col. 5, lines 62-65 and col. 6, lines 12-17);
- A data bus connected to said operation processing unit and said memory (col. 5, lines 3-10); and
- A pseudo-data generating circuit connected to said data bus (col. 11, lines 14-18), said pseudo-data generating circuit which generates pseudo-data and outputs the pseudo-data to said memory to cause instruction to randomly execute (col. 11, lines 22-25).

Ugon does not teach the pseudo-data generating circuit outputs the pseudo-data to said data bus in a time interval between the read cycle period and the write cycle period, between the write cycle period and the read cycle period, between two read cycle periods, or between two write cycle periods.

However, Feyt et al. discloses a method for hiding operation performed by the microprocessor card by presenting random data items on the data bus during cryptographic calculations; cryptographic calculations require reading and writing operations to be performed by the processor (col. 2, lines 36-42 and col. 3, lines 34-52).

Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify the Ugon system with the teaching of Feyt et al. to output pseudo-data on the data bus between read and write cycles. One would be motivated to do so in order to mask the power consumption by the memory during the reading or writing of secret data to prevent an attacker from deducing the data by correlation or differential power analysis attacks (col. 1, lines 36-46).

Regarding claims 2, 4, 12 and 14, Ugon as modified by Feyt et al. teaches wherein said pseudo-data generating circuit generates random number data as the pseudo-data (see col. 11, lines 14-18 and col. 12, lines 34-37 of Ugon).

**(10) Response to Argument**

Appellant argues that Feyt et al. does not teach outputting random data to the data bus provided between the central unit and the memory.

First, Ugon teaches a processor (fig. 1, ref. num 1), memory (fig. 1, ref. num 12), and a data bus (fig. 1, ref. num 3). In addition, registers 1, 2, and 3 (fig. 1, R1, R2, R3), along with interrupt (fig. 1, ref. num 15) provide random interrupts (data) to the data bus, which cause the data to appear at random times, instead of all at once, so power analysis cannot properly occur.

Second, Feyt et al. teaches a processor (fig. 1, ref. num 12), memory (fig. 1, ref. num 14), and a data bus (col. 3, lines 20-23 and lines 42-43). In addition, a random signal generator (fig. 1, ref. num 28) is used to provide randomness to the power consumption of the processor and memory so power analysis cannot properly occur.

Ugon does not teach that the registers and interrupt provide randomness during time intervals between read cycles, write cycles, or read and write cycles (as claimed in the independent claims). Feyt et al. discloses (at column 3, lines 33-53, specifically, step 5) that in order to mask the power consumption of a cryptographic calculation (in order to prevent hacking by power analysis), the cryptographic calculations take place during step 5, which is after a write cycle. As is known, a processor performs many cycles, and therefore performs additional read and write cycles after the step 5 write cycle. This shows that pseudo-data is generated between read cycles, write cycles, and/or read & write cycles.

**(11) Related Proceeding(s) Appendix**

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Brandon Hoffman

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Conferees:

Christopher Revak

Gilberto Barron